



- (51) International Patent Classification:
H04L 29/12 (2006.01) *H04L 29/08* (2006.01)
- (21) International Application Number:
PCT/US2016/038556
- (22) International Filing Date:
21 June 2016 (21.06.2016)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
14/752,716 26 June 2015 (26.06.2015) US
- (71) Applicant: WESTERN DIGITAL TECHNOLOGIES, INC. [US/US]; 3355 Michelson Drive, Suite 100, Irvine, California 92612 (US).
- (72) Inventors: BJORNSON, Eric S.; 550 Dawn Drive, Sunnyvale, California 94087 (US). BATRA, Rajesh K.; 1590 Montebello Oaks Court, Los Altos, California 94024 (US). JOSE CHIRIYANKANDATH, Cipson; 3355 Michelson Drive, Suite 100, Irvine, California 92612 (US).
- (74) Agents: TRUESDALE, Sabra-Anne et al.; Western Digital Technologies, Inc., 3355 Michelson Drive, Suite 100, Irvine, California 92612 (US).
- (81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,

[Continued on next page]

(54) Title: AUTOMATIC DISCOVERY AND ONBOARDING OF ELECTRONIC DEVICES

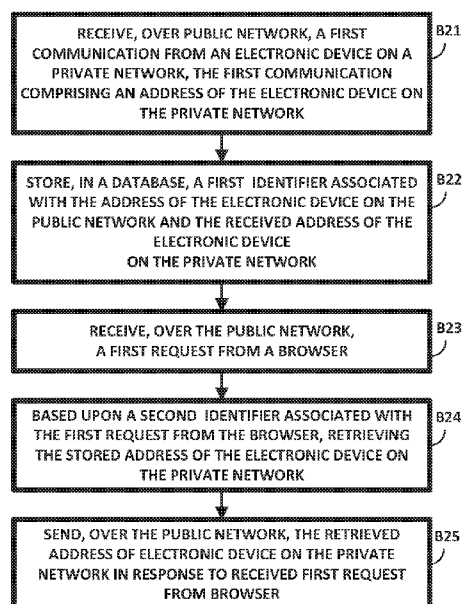


FIG. 2

(57) Abstract: A computing device configured to facilitate on-boarding of an electronic device may comprise a processor and memory. The memory may store instructions that cause the processor to receive, over a public network, a first communication from the electronic device on a private network, comprising an address of the electronic device on the private network. A first identifier associated with the address of the electronic device on the public network and the received address of the electronic device on the private network may be stored in a persistent store. The computing device may then receive a first request from a browser and, based upon a second identifier associated therewith, retrieve the stored address of the electronic device on the private network. The retrieved address of the electronic device on the private network may then be sent, over the public network, in response to the received first request from the browser.



SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

— *with international search report (Art. 21(3))*

AUTOMATIC DISCOVERY AND ONBOARDING OF ELECTRONIC DEVICES

BACKGROUND

[0001] Embodiments are related to configuring an electronic device for use on a network. In particular, embodiments are related to configuring a data storage device such as a Network Attached Storage (NAS) on a Local Area Network (LAN), such as may occur when the user firsts connects a new data storage device to his or her LAN.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] Fig. 1 is a block diagram of a system according to one embodiment.

[0003] Fig. 2 is a flow chart of a method according to one embodiment.

DETAILED DESCRIPTION

[0004] Many devices that are configured to operate in computer networks have no or very limited user interfaces. For example, data storage devices such as network attached storage (NAS) computing devices typically do not comprise a display or a keyboard that would enable a user to perform the initial device setup, a process that is also called on-boarding. Currently, the user migrates data to his or her new NAS using a dedicated application that is at least initially stored on the NAS. This can be cumbersome and puts the user in an unfamiliar environment. Users are, however comfortable with using web browsers to carry out a great many tasks. However, detecting electronic devices in a local network from a sandboxed environment (e.g., a protocol-restricted and security-constrained environment) such as a web browser may be difficult. Indeed, in order to perform the initial setup process to enable access to and use of the electronic device on the local network, the electronic device must first be detected on the local network using the web browser.

[0005] It is critical for a user's newly-purchased device (or an existing device moved to a new network) to be reliably discovered and accessed on the network. If this is not the case, the device is effectively invisible on the network and might as well be non-existent. Device auto-discovery, at least on mobile devices, is

conventionally carried out via Bonjour or other network technologies, which provides a general method to discover services on a local area network. Digital Living Network Alliance (DLNA) is one example of such network technologies. DLNA defines interoperability guidelines to enable sharing of digital media between multimedia devices, media management, discovery and control. Such device/service discovery technologies are used for service discovery, address assignment, and hostname resolution. However, they are based on broadcast technologies and can be disabled using router configurations, and thus reducing the reliability of device discovery. There is no reliable technology that is both technology and platform independent that allows any applications including the sandboxed applications such as browsers to reliably detect interested devices in the local network.

[0006] Fig. 1 is a block diagram of a system according to one embodiment. As shown therein, an electronic device 102 may be coupled to a private network (e.g., a user's local area network (LAN)) 101. The electronic device 102 may be coupled to the private network 101 through a wired or wireless connection. In one implementation, the electronic device 102 may comprise a NAS, a Storage Attached Network (SAN) a redundant array of inexpensive disks (RAID), or most any network-aware electronic device. Alternatively, electronic device 102 may be any network aware device embedded with electronics, software, sensors and connectivity to enable it to exchange data with the manufacturer, operator and/or other connected devices. The electronic device 102 may be uniquely identifiable through its embedded computing system and may be configured to interoperate within an existing network infrastructure, including LAN 101 and a wide area network (WAN) such as the Internet.

[0007] The electronic device 102 may be coupled to a networking device such as a router 104, configured to forward data packets between LAN 101 and the WAN 106. Other devices may be located on the LAN 101 such as, for example, computing device 114. Computing device 114 may comprise a computer and a display. The computing device may take many forms including, for example, a tablet computer, a desktop computer, a laptop computer or a mobile device such as a smartphone. The computing device 114 may be configured to run a browser, such as shown at 116 in Fig. 1.

[0008] A remote coordinating server 108 may be coupled to the WAN 106. The remote coordinating server 108 may comprise of one or more physical and/or virtual computing devices and may be implemented at least partially in hardware and/or software. According to one embodiment, the remote coordinating server 108 may include mass storage. The mass storage, according to one embodiment, may comprise a Hard Disk Drive (HDD) 118 comprising one or more rotating magnetic disks. The mass storage of the remote coordinating server 108 may also or alternatively include non-volatile (e.g., Flash-based) memories 120. Alternatively still, the mass storage of the remote coordinating server 108 may comprise one or more hybrid storage devices 119, each comprising both magnetic disks 118 and non-volatile semiconductor memory 120. As also shown in Fig. 1, the remote coordinating server 108 may comprise one or more microprocessor 122, coupled to the mass storage, to a memory 124 and to a network interface 126. The microprocessor(s) 122 may be configured to execute instructions configured to implement an embodiment, as described herein relative to Figs. 1 and 2.

[0009] On-boarding may refer to or comprise the process of customizing the generalized software available in off-the-shelf electronic devices (such as NASs) to user preference. One embodiment makes use of remote coordinating server 108 to collect information from the electronic device and/or a client computing device 124 to prepopulate many of the onboarding information fields, to enable the user to quickly and efficiently finish the onboarding process. Indeed, one embodiment allows sandboxed applications such as web browser 116 to use networking protocols in association with a remote coordinating server such as shown at 108 to automatically and accurately detect and on-board electronic devices such as 102 in a private network such as LAN 101. This process, according to one embodiment, results in newly-connected and accessible electronic device 102 sending identity information to remote coordinating server 108, thereby enabling the remote coordinating server 108 to register the electronic device 102 on the network and render it accessible to the user. One embodiment enables the remote coordinating server 108 to pull required information directly from the electronic device 102 and to allow the user to request details of the electronic device 102 from the browser 116. Thereafter, the web browser 116 can facilitate the on-boarding of the electronic device through, for example,

prepopulating the electronic device 102 using information retrieved from the electronic device 114 and/or from the remote coordinating server 108.

[0010] According to one embodiment, the electronic device 102 in the private network 101 may send, via networking device 104, a first communication to the remote coordinating server 108 on the WAN 106. This first communication may comprise the address of the electronic device on the private network 101. This address may be an address on the LAN 101 such as, for example, 192.168.0.10, which is an address that is only valid on the LAN 101. This first communication may have been sent by the electronic device to the remote coordinating server 108 because the electronic device is a newly-purchased electronic device that is newly coupled to the LAN 101. Alternatively, the electronic device 102 may be a previously used device that is connected for the first time to the private network 101. Alternatively still, the electronic device 102 may be a pre-existing device on the local area network, but at a new address. According to another embodiment, the electronic device 102 may periodically (or responsive to a predetermined event) send the first communication containing its address on the LAN 101 to the remote coordinating server 108, for any reason.

[0011] Upon receipt of the first communication from the electronic device 102, the remote coordinating server 108 may store, in a persistent store 109 (such as, for example, a database or a memcache), a first identifier associated with the address of the electronic device on the public network (such as WAN 106) and the received address of the electronic device on the private network 101. The persistent store 109 may be within the remote coordinating server 108, coupled thereto or otherwise accessible thereto over a computer network such as shown at 106. Alternatively, the persistent store 109 may be within the same data center as the remote coordinating server and may be accessible over a LAN. The remote coordinating server 108 may extract the address of the router 104 from the packets of the first communication issued by the electronic device 102. This extracted address may be or include the Internet Protocol (IP) address of the router 104. The remote coordinating server may also store, in the persistent store 109, the address of the electronic device 102 in the LAN 101 (or an encrypted version thereof), which address was at least part of the payload of the packets of the first communication received by the remote coordinating

server 108. According to one embodiment, the remote coordinating server 108 may store the private address(es) of the electronic device(s) 102 in the private network 101 in a record (e.g., in a row or rows of a database, key value of a memcache) of the persistent store 109 associated with or related to the public address of the electronic device on the public network 106. The stored public address of the electronic device 102 on the public network 106 may, therefore, act as an index or key into the persistent store 109 to retrieve therefrom the corresponding private address(es) (which may be encrypted) of the electronic devices 102 on the private network 101.

[0012] According to one embodiment, this first communication may be auto-generated by the electronic device 102 upon detecting a triggering event such as, for example, being newly-connected to private network 101. The electronic device 102 may, according to one embodiment, have prior knowledge of the remote coordinating server 108 and its IP address on the WAN 106. For example, the remote coordinating server 108 may have been configured by the manufacturer of the electronic device 102 and the address thereof may have been pre-loaded onto the electronic device 102 to allow just such auto-generated first communication to the remote coordinating server 108. Indeed, such first communication, according to one embodiment, may be carried out well before any on-boarding attempt is carried out, via the browser 116 of computing device 114 or otherwise.

[0013] Sometime later, perhaps when the user has initiated the on-boarding procedure, the remote coordinating server may receive, over the public network 106, a first request from browser 116 running on computing device 116. It is to be noted that the computing device 116 is a different device than electronic device 102. Such first request, issued by browser 116 and received by remote coordinating server 108, may be characterized as a first on-boarding request; that is, a request intended to at least initiate the on-boarding procedure of the electronic device 102 on the private network 101. It is to be noted that the first request is passed between private network 101 and public network 106 via the router 104.

[0014] Based upon a second identifier associated with the first request from the browser 116, the remote coordinating server 108 may retrieve the previously-stored private address or addresses of the electronic device or devices 102 on the

private network 101. In this regard, it is to be noted that the packets of this first request from browser 116 include the same public address as did the packets of the previously sent and received first communication from the electronic device 102 to the remote coordinating server 108. According to one embodiment, therefore, the second identifier may be or may be related to this same public address. According to one embodiment, the remote coordinating server 108 may extract, from the first request received from the browser 116, the public IP address of the computing device 114, which is the public IP address of the router 104, which is the same networking device, at the same public address, that routed the packets of the prior first communication from the electronic device 102 to the remote coordinating server 108. In this manner, the remote coordinating server 108 may use the public address extracted from this received first request to index into the persistent store 109 and to retrieve therefrom the private address of the electronic device 102 in the private network 101, which private address was previously stored in a record of persistent store 109 corresponding to or associated with the public address extracted from first request (and previously extracted from the first communication from the electronic device 102 to the remote coordinating server 108). Now in possession of the retrieved private address of the electronic device 102 and responsive to the received first request from the browser 116, the remote coordinating server 108 may send this retrieved private address, over the public network 116 to the browser 116 as well as, optionally, additional information such as product model and device name, for example. In the case in which there are multiple devices that are found for the same public IP address, this information may be useful to enable the user to easily select the proper device. This retrieved private address may require decryption if previously encrypted. The browser 116, and thus the computing device 114, is now in possession of the private address of the electronic device 102 and may initiate or continue the on-boarding procedures to fully configure and allow access to the electronic device, over both the public network 106 and the private network 101.

[0015] According to one embodiment, the first identifier extracted by the remote coordinating server 108 from the first communication received from the electronic device may be or may include the address of the electronic device 102 (e.g., that of the router 104) on the public network 106. For privacy, however, this first

identifier may be or may comprise a hash of the address of the electronic device 102 on the public network 106. Similarly, the second identifier extracted from the first request received from browser 116 by the remote coordinating server 108 may be or may comprise the address of the computing device 114 (e.g., that of the router 104) on the public network 106. For privacy, however, this second identifier may be an encrypted or obfuscated version of the address of the computing device 104 on the public network 106. To enable the remote coordinating server 108 to index into the persistent store 109 using the second identifier, the hashing algorithm used to scramble the public address extracted from the first communication from the electronic device 102 may be the same hashing algorithm as that used to scramble the public address extracted from the first request received from the browser 116 of computing device 114. If different hashing algorithms are used to scramble the extracted public addresses, a mechanism should be instituted to enable the remote coordinating server 108 to associate one with the other, to enable the remote coordinating server to index into the persistent store, to identify the record in which the private address of the electronic device 102 is stored and to retrieve that private address and provide the same to the computing device 114 responsive to the first request from the browser 116.

[0016] According to one embodiment, the first communication received by the remote coordinating server 108 from the electronic device 102 may comprise or contain more than just the private address of the electronic device 102 on the private network 101. Indeed, according to one embodiment, this first communication may also contain a third identifier of the electronic device, a name of the electronic device and/or select characteristics of the electronic device 102. This third identifier may be human-observable. Examples of human-observable third identifiers may include, for example, a serial number of the electronic device 102 or any other identifier such as a Media Access Control (MAC) address of the electronic device and/or any other human-perceptible indication printed on the device or the packaging thereof. The select characteristics of the electronic device may comprise selected items from the electronic device's specifications and/or any other characteristics that may be useful in on-boarding and/or otherwise configuring the electronic device 102 for access and use. Such third identifier, name and/or select characteristics contained in the first

communication from the electronic device 102 to the remote coordinating server 108 may also be stored in the persistent store 109 at a location associated with the (optionally hashed) public address extracted from the first communication from the electronic device 102 and accessed using the matching public address (also optionally hashed or otherwise scrambled or obfuscated) extracted from the first request from the browser 116.

[0017] According to one embodiment, the information sent by the electronic device 102 to the remote coordinating server 108 may be updated. Indeed, according to one embodiment, the remote coordinating server 108 may be further configured to receive, over public network 106, a second communication from the electronic device 102 on the same private network 101 or on another private network. The second communication may comprise an updated private address of the electronic device 102 on the private network 101 or on the other private network. Upon receipt of this second communication, the remote coordinating server 108 may store, in the persistent store 109, an updated first identifier associated with the updated address of the electronic device 102 on the public network 106 (which may be the same or different from the previously-stored first identifier) and the received updated address of the electronic device 102 on the private network 101 or on the other private network. This second communication from the electronic device 102 to the remote coordinating server 108 may be carried out by the electronic device 102 automatically; that is, without human intervention.

[0018] The remote coordinating server 108 may, at some later time, receive receiving, over the public network 106, a second request from the browser 116 (or from another browser running on computing device 114 or on another computing device). Based upon an updated second identifier associated with the second request from the browser 116 or another browser, the remote coordinating server 108 may retrieve from the persistent store 109 the stored updated private address of the electronic device 102 on the private network 101 or some other private network. The updated second identifier may be or may comprise the extracted public address of the electronic device 102 on the public network 106, or a hash or a scrambled or otherwise obfuscated version thereof. In response to the received second request from the browser 116 or the other browser, the remote coordinating server 108 may then send,

over the public network 106; the retrieved updated address of the electronic device 102 on the private network 101 or on the other private network, as well as additional information such as, for example, the device name and product model.

[0019] If this process fails to register the electronic device 102 (such as a NAS) with the remote coordinating server 108, the user may log onto the server's website ((e.g., MyCloud.com in the case in which the remote coordinating server is a Western Digital Corp. server), and manually register and on-board his or her electronic device 102 through a guided setup procedure. According to one embodiment, the remote coordinating server 108 may provide code (such as JavaScript, for example), which may be executed within the browser to scan devices on the user's private network 101 for default names with which the remote coordinating server knows the electronic device 102 may be initially configured.

[0020] According to one embodiment, therefore, when in the user's private network (e.g., LAN) environment, the electronic device 102 may send (in a first communication) its identify information, including IP address, MAC address, name, serial number and/or other pieces of information to a remote coordinating server 108 over a WAN 106. The remote coordinating server 108 may then detect this registration request and may then register the electronic device 102 in its persistent store 109, with the identity information and the network routing details. When the user later connects, in a first request, to a designated Universal Resource Locator (URL) (e.g. MyCloud.com) from a browser 116, the user may then be automatically presented with website that is personalized to his or her electronic device information. This website may be at the remote coordinating server 108 or at some other location, and may already be personalized with the serial number, name and/or MAC address (among other possibilities) of his or her electronic device 102. From this personalized website, the user may complete the device configuration and/or initial setup process using the familiar web browser 116, to complete the onboarding process via communications between the browser 116 and the electronic device 102. The user and/or the remote coordinating server or other authorized users may then access the electronic device 102 over the WAN 106 or LAN 101, based on network availability. Likewise, the remote coordinating server 108 may then also pull data from the electronic device 102 and provide the user with, for example, a listing of all shares, files, directories, histories

of upload, downloads, etc. Alternatively, other clients (e.g., an app on a mobile device) may then pull data from the electronic device 102.

[0021] According to an embodiment, any changes in the user's local network, such as a change to the public or private IP address of the electronic device 102 may be timely communicated to the remote coordinating server 108. Similarly, any changes in the identity of the electronic device such as device name or device capability may also, according to one embodiment, be communicated to the remote coordinating server 108 in a timely manner, without user intervention. Also, any change in the public IP address of the router 104 to which the electronic device 102 is connected may also be automatically communicated to the remote coordinating server 108. To help ensure privacy and to avoid data breaches, in one embodiment, some or all of the information passed through the remote coordinating server 108 may be hashed and/or otherwise anonymized. Moreover, communications to the remote coordinating server 108 may be further validated with unique headers, to further reduce potential external threats. Alternatively, other methods and protocols may be used (such as HTTPS, for example) to provide authentication, validation and/or other services.

[0022] Fig. 2 is a flow chart of a method according to one embodiment. As shown therein, block B21 calls for receiving, over a public network, a first communication from an electronic device on a private network. As detailed above, the first communication may comprise at least an address of the electronic device on the private network. As shown in block B22, the method may further comprise storing, in a persistent store, a first identifier associated with the address of the electronic device on the public network and the received address of the electronic device on the private network. At some later time, as shown at B23, the remote coordinating server 108 may receive, over the public network, a first request from a browser. It is to be understood that the browser runs on a computing device that is different than the electronic device. Thereafter, based upon a second identifier associated with the first request from the browser, the remote coordinating server may retrieve the stored address(es) of the electronic device(s) on the private network, as shown at B24. Lastly, block B25 calls for sending, over the public network; the retrieved address of the electronic device on the private network in response to the received first request

from the browser. The user may now manage his or her newly-discovered, registered and configured electronic device through the familiar environment of his or her web browser.

[0023] Another embodiment is a data storage device such as the NAS 102 depicted in Fig. 1. Such a NAS 102 may comprise memory 1022 storing a public network address for a remote coordinating server and an identifier for the NAS, a network interface 1023 and one or more processors 1021. The processor(s) 1021, according to one embodiment, may be configured to during an initial setup process on a private network, determine the private network address of the NAS 102 and transmit the private network 101 address and the identifier to the remote coordinating server, with the remote coordinating server 108 is located on a public network 106 (that is different from the private network 101). A network communication may be received, at the private network address of the NAS 102, from a computing device 114 on the private network 101, with the private network address having been obtained by the computing device 114 from the remote coordinating server 108. In response to receiving the network communication from the computing device (or some time thereafter), the NAS 102 may provide an interface (for displaying an end user license, to enable configuration information to be entered, etc.) to the computing device 114. The NAS 102 may then be configured using the interface from user input and/or may be at least partially automatically or programmatically configured. For example, the one or more processors 1021 may be further configured to pre-populate fields corresponding to the language of the requesting browser, the time zone in which the NAS resides and/or the current time, among many possibilities. Such information may have been obtained from the electronic device 114, from the coordinating server 108 and/or from other sources.

[0024] According to one embodiment, the method provides an intuitive and automatic pathway for on-boarding of NASs and other electronic device that does not require the user to manually register his or her device on the network, thereby taking this complexity away from the user and rendering the process of onboarding an electronic device a seamless process. Advantageously, the present device discovery mechanism according to one embodiment works without necessitating or relying on the use of network broadcast technologies such as Bonjour or DLNA. These

technologies may have limited effectiveness due to router behavior or browser constraints, as most of the modern routers may readily be configured to disallow broadcasting for security and performance reasons. Although embodiments have been presented herein in terms of network attached storage devices, other electronic devices may be on-boarded according to embodiments. For example, the embodiments shown and described herein may be practiced to good advantage on or with other types of networked devices with limited input capability such as, for example, IP telephones, routers, switches, access points, networked-TV tuners, etc.

[0025] Moreover, according to one embodiment, no modification and/or installation of new software is required on the computing device 114 in order to perform the setup of, configure or on-board the NAS or other electronic device. Indeed, the computing device 114 may be configured to communicate with the electronic device 102 using pre-existing software installed on the computing device 114 prior to the initial setup process.

[0026] Herein, the use of ordinal qualifiers such as “first”, “second”, “third” is not necessarily intended to connote sequentiality or any particular ordering. Rather, such qualifiers may be interpreted solely as distinguishing one quantity from another.

[0027] While certain embodiments of the disclosure have been described, these embodiments have been presented by way of example only, and are not intended to limit the scope of the disclosure. Indeed, the novel methods, devices and systems described herein may be embodied in a variety of other forms. Furthermore, various omissions, substitutions and changes in the form of the methods and systems described herein may be made without departing from the spirit of the disclosure. The accompanying claims and their equivalents are intended to cover such forms or modifications as would fall within the scope and spirit of the disclosure. For example, those skilled in the art will appreciate that in various embodiments, the actual physical and logical structures may differ from those shown in the figures. Depending on the embodiment, certain steps described in the example above may be removed, others may be added. Also, the features and attributes of the specific embodiments disclosed above may be combined in different ways to form additional

embodiments, all of which fall within the scope of the present disclosure. Although the present disclosure provides certain preferred embodiments and applications, other embodiments that are apparent to those of ordinary skill in the art, including embodiments which do not provide all of the features and advantages set forth herein, are also within the scope of this disclosure. Accordingly, the scope of the present disclosure is intended to be defined only by reference to the appended claims.

CLAIMS:

1. A computer-implemented method, comprising:

receiving, over a public network, a first communication from an electronic device on a private network, the first communication comprising an address of the electronic device on the private network;

storing, in a persistent store, a first identifier associated with the address of the electronic device on the public network and the received address of the electronic device on the private network;

receiving, over the public network, a first request from a browser running on a computing device that is different than the electronic device;

based upon a second identifier associated with the first request from the browser, retrieving the stored address of the electronic device on the private network; and

sending, over the public network; the retrieved address of the electronic device on the private network in response to the received first request from the browser.

2. The computer-implemented method of claim 1, wherein the first identifier comprises one of address of the electronic device on the public network and a hash of the address of the electronic device on the public network.

3. The computer-implemented method of claim 1, wherein the second identifier comprises one of the address of the electronic device on the private network and an encrypted version of the address of the electronic device on the private network.

4. The computer-implemented method of claim 1, wherein the first communication received from the electronic device further comprises at least one of a third identifier of the electronic device, a name of the electronic device and select characteristics of the electronic device.

5. The computer-implemented method of claim 4, wherein the third identifier is human-observable.

6. The computer-implemented method of claim 4, wherein storing further comprises storing, in the persistent store, the at least one of the identifier of the

electronic device, the name of the electronic device and the select characteristics of the electronic device.

7. The computer-implemented method of claim 1, wherein retrieving comprises matching the second identifier associated with the first request from the browser with the stored first identifier associated with the address of the electronic device on the public network and, upon determining a match, retrieving the address of the electronic device on the private network stored in a record of the persistent store associated with the matching first and second identifiers.

8. The computer-implemented method of claim 1, wherein the electronic device comprises a data storage device.

9. The computer-implemented method of claim 1, further comprising:
receiving, over a public network, a second communication from the electronic device on the private network or an other private network, the second communication comprising an updated address of the electronic device on the private network or on the other private network;

storing, in the persistent store, an updated first identifier associated with the updated address of the electronic device on the public network and the received updated address of the electronic device on the private network or on the other private network;

receiving, over the public network, a second request from the browser or an other browser

based upon an updated second identifier associated with the second request from the browser or the other browser, retrieving the stored updated address of the electronic device on the private network or on the other private network; and

sending, over the public network; the retrieved updated address of the electronic device on the private network or on the other private network in response to the received second request from the browser or the other browser.

10. A computing system, comprising:

a network interface;

one or more processors configured to:

receive, over a public network, a first communication from an electronic device on a private network, the first communication comprising an address of the electronic device on the private network;

store, in a persistent store, a first identifier associated with the address of the electronic device on the public network and the received address of the electronic device on the private network;

receive, over the public network, a first request from a browser running on a computing device that is different than the electronic device;

based upon a second identifier associated with the first request from the browser, retrieve the stored address of the electronic device on the private network; and

send, over the public network, the retrieved address of the electronic device on the private network in response to the received first request from the browser.

11. The computing system of claim 10, wherein the first identifier comprises one of the address of the electronic device on the public network and a hash of the address of the electronic device on the public network.

12. The computing system of claim 10, wherein the second identifier comprises one of the address of the electronic device on the private network and an encrypted version of the address of the electronic device on the private network.

13. The computing system of claim 10, wherein the first communication received from the electronic device further comprises at least one of a third identifier of the electronic device, a name of the electronic device and select characteristics of the electronic device.

14. The computing system of claim 13, wherein the third identifier is human observable.

15. The computing system of claim 13, wherein the stored instructions are further configured to cause the processor to store, in the persistent store, the at least one of the identifier of the electronic device, the name of the electronic device and the select characteristics of the electronic device.

16. The computing system of claim 10, wherein the stored instructions are

further configured to cause the processor to match the second identifier associated with the first request from the browser with the stored first identifier associated with the address of the electronic device on the public network and, upon determining a match, retrieve the address of the electronic device on the private network stored in a record of the persistent store associated with the matching first and second identifiers.

17. The computing system of claim 10, wherein the electronic device comprises a data storage device.

18. The computing system of claim 10, wherein the stored instructions are further configured to cause the processor to:

receive, over a public network, a second communication from the electronic device on the private network or an other private network, the second communication comprising an updated address of the electronic device on the private network or on the other private network;

store, in the persistent store, an updated first identifier associated with the updated address of the electronic device on the public network and the received updated address of the electronic device on the private network or on the other private network;

receive, over the public network, a second request from the browser or an other browser

based upon an updated second identifier associated with the second request from the browser or the other browser, retrieve the stored updated address of the electronic device on the private network or on the other private network; and

send, over the public network; the retrieved updated address of the electronic device on the private network or on the other private network in response to the received second request from the browser or the other browser.

19. A network attached electronic device, comprising:

memory storing a public network address for a remote coordinating server and an identifier for the electronic device; and

one or more processors configured to:

during an initial setup process on a private network, determine a private

network address of the electronic device and transmit the private network address and the identifier to the remote coordinating server, wherein the remote coordinating server is located on a public network different from the private network;

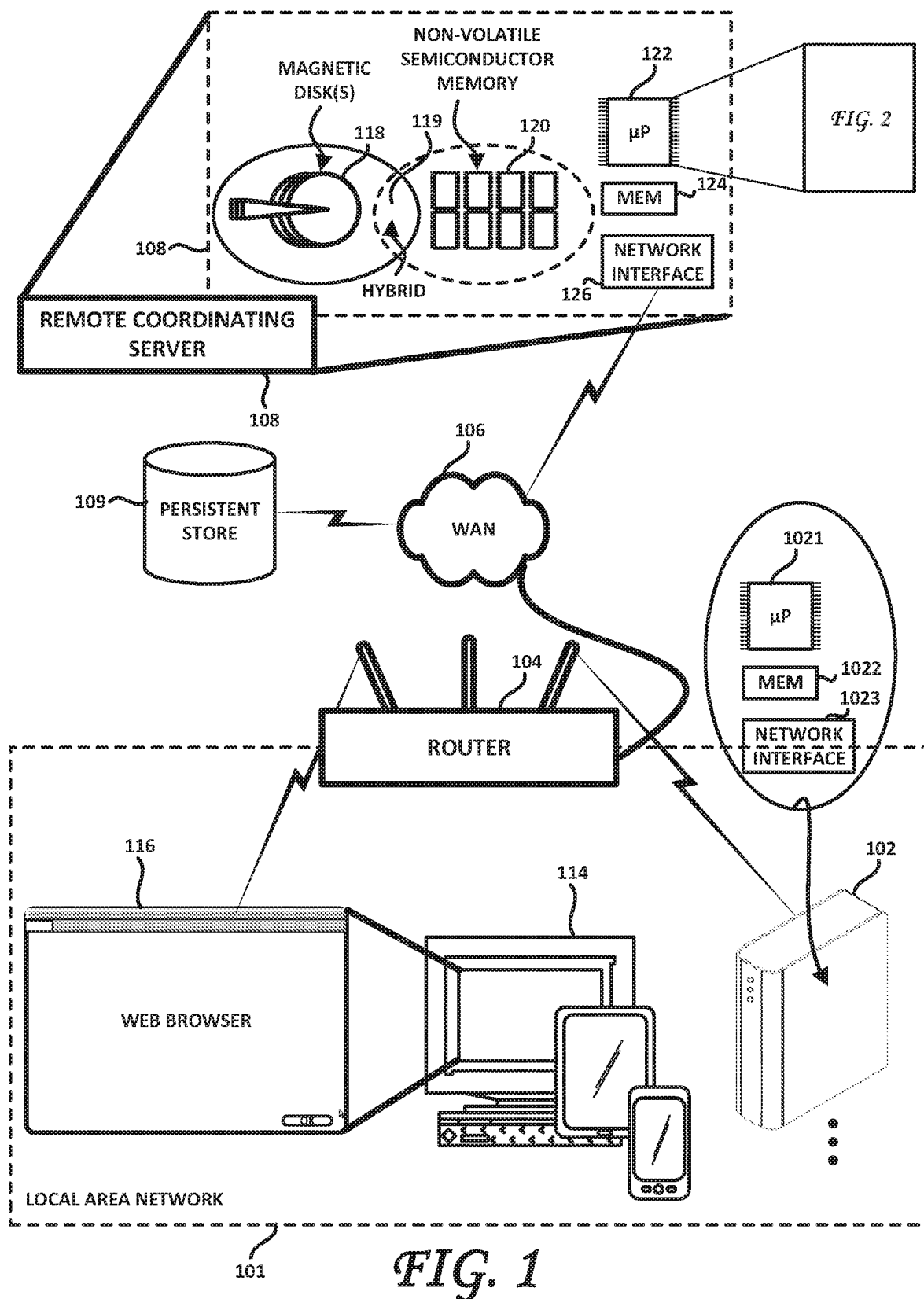
receive, at the private network address of the electronic device, a network communication from a computing device on the private network, wherein the private network address was obtained by the computing device from the remote coordinating server; and

in response to receiving the network communication from the computing device, provide an interface for the electronic device to the computing device.

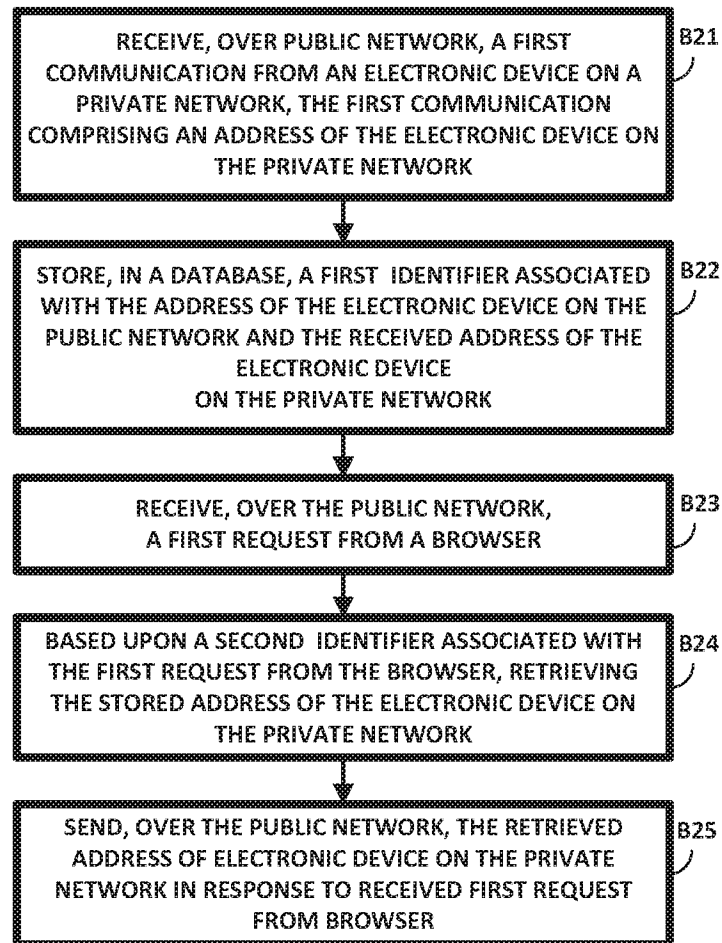
20. The electronic device of claim 1, wherein the one or more processors are further configured to pre-populate at least one of language, time zone and time information in the electronic device from information obtained from the computing device.

21. The electronic device of claim 1, wherein the computing device is configured to communicate with the electronic device using pre-existing software installed on the computing device prior to the initial setup process.

1/2



2/2

*FIG. 2*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2016/038556**A. CLASSIFICATION OF SUBJECT MATTER****H04L 29/12(2006.01)I, H04L 29/08(2006.01)I**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 29/12; G06F 15/16; G06F 15/173; H04L 29/00; H04W 88/18; G06Q 50/00; H04W 28/10; G06Q 50/26; H04L 29/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: electronic device, persistent store, computing device, address, public network, private network

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 02-102012 A2 (4TH PASS INC.) 19 December 2002 See page 25, lines 24-29; claims 1, 2, 73; and figure 7.	1-18
Y		19-21
Y	US 6993595 B1 (GREGORY LUPTOWSKI et al.) 31 January 2006 See column 5, lines 25-32; and figure 2A.	19-21
A	KR 10-2003-0096532 A (INFORBANK CORPORATION) 31 December 2003 See claims 6-7; and figure 8.	1-21
A	KR 10-2012-0029082 A (NEOWIZ GAMES CORP.) 26 March 2012 See paragraph [0099]; and figure 10.	1-21
A	WO 2014-077457 A1 (CDNETWORKS CO., LTD.) 22 May 2014 See paragraphs [112]-[121]; and figure 3.	1-21



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

06 September 2016 (06.09.2016)

Date of mailing of the international search report

21 September 2016 (21.09.2016)

Name and mailing address of the ISA/KR

International Application Division

Korean Intellectual Property Office

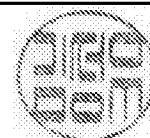
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea

Facsimile No. +82-42-481-8578

Authorized officer

KIM, Seong Woo

Telephone No. +82-42-481-3348



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2016/038556

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 02-102012 A2	19/12/2002	AT 328436 T AU 2002-345633 A1 CN 1528081 A DE 60211897 D1 DE 60211897 T2 EP 1400093 A2 EP 1400093 B1 ES 2263791 T3 JP 2004-533190 A KR 10-2004-0034612 A US 2003-0028671 A1 WO 02-102012 A3	15/06/2006 23/12/2002 08/09/2004 06/07/2006 19/10/2006 24/03/2004 31/05/2006 16/12/2006 28/10/2004 28/04/2004 06/02/2003 03/04/2003
US 6993595 B1	31/01/2006	None	
KR 10-2003-0096532 A	31/12/2003	None	
KR 10-2012-0029082 A	26/03/2012	KR 10-1193345 B1	26/10/2012
WO 2014-077457 A1	22/05/2014	CN 104380789 A EP 2922338 A1 JP 2016-506104 A KR 10-1491638 B1 KR 10-2014-0062954 A US 2014-0330942 A1	25/02/2015 23/09/2015 25/02/2016 09/02/2015 27/05/2014 06/11/2014